Encryption communication system for generating passwords on basis of star information on both parties of communication

Patent number:	CN1199892
Publication date:	1998-11-25
Inventor:	FUKAWA YASUROU (JP)
Applicant:	ANY CO LTD (JP)
Classification:	
- international:	G06F7/58
- european:	G07F7/10D4E2; G07F7/10E; H04L9/22
Application number:	CN19980109269 19980520
Priority number(s):	JP19970129405 19970520

Also published as:

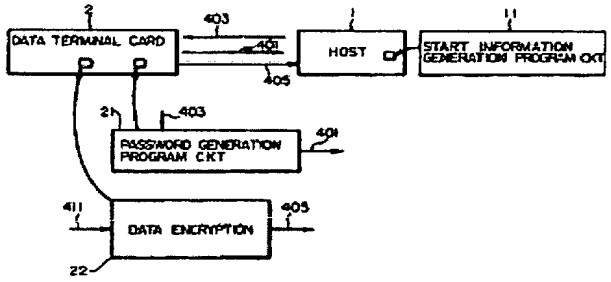
EP0880115 (A2
US6112187 (A1
JP10322327 (A
EP0880115 (A3
EP0880115 (B1

more >>

Abstract not available for CN1199892
Abstract of corresponding document: **EP0880115**

An encryption communication system including a host (1) and a data terminal card device (2) is disclosed. The host (1) includes a start information generation program circuit (11) for generating password generation start information which has not been used in the past. When the data terminal card device (2) is connected to the host (1) for communication, a password generation program circuit (21) included in the card device (2) generates a password in accordance with the start information received from the host (1). The card device (2) sends the generated password to the host (1) for certification. If the received password is coincident with a password generated in the host (1), the host certifies the received password and allows communication to be held. An encryption circuit (22) also included in the card device (2) controls a plurality of different encryption programs in a sophisticated way so as to execute time-varying irregular control, thereby generating encrypted data.

Fig. 1



[19]中华人民共和国专利局

[51]Int.Cl[6]
G06F 7/58

[12] 发明专利申请公开说明书

[21] 申请号 98109269.1

[43]公开日 1998 年 11 月 25 日

[11] 公开号 CN 1199892A

[22]申请日 98.5.20

[30]优先权

[32]97.5.20 [33]JP[31]129405／97

[71]申请人 安尼株式会社

地址 日本神奈川县

[72]发明人 府川泰朗

[74]专利代理机构 中国专利代理(香港)有限公司

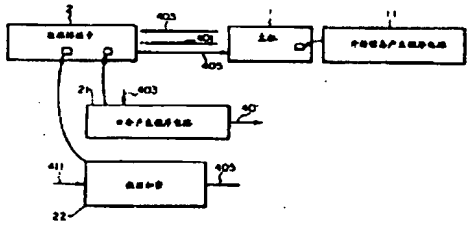
代理人 吴增勇 张志醒

权利要求书 6 页 说明书 17 页 附图页数 16 页

[54]发明名称 根据通信双方的开始信息产生口令的加密通信系统

[57]摘要

包括主机和数据终端卡装置的加密通信系统。主机包括开始信息产生程序电路，用来产生过去没有用过的口令产生开始信息。当数据终端卡装置与主机通信时，包括在数据终端卡装置中的口令产生程序电路按照从主机接收的开始信息产生口令。卡装置把产生的口令发送给主机来确认。若接收的口令与主机中产生的口令一致，则主机确认接收的口令，并允许通信继续保持。在卡装置中还包括加密电路，它以复杂的方式控制多个不同的加密程序，以此产生加密的数据。



权 利 要 求 书

1.一种加密通信系统，其特征在于包括:

第一通信装置，用来产生用于生成每次通信连接都不相同的口令的有意义的信息；和

第二通信装置，用来根据从第一通信装置接收到的信息产生基于所述信息的口令，并将所述口令送到第一通信装置;

所述第一通信装置包括：

信息产生电路，用来根据一种不规则的信号产生所述信息;

第一口令生成器，用来根据所述信息利用口令产生程序产生口令;

判决电路，用来确定从所述第二通信装置接收到的口令是否与从所述第一口令产生电路输出的口令一致，若两口令一致则输出一致信号，而若它们不一致则输出不一致信号;

第一通信开始电路，用来响应一致信号开始与第二通信装置的加密通信;

所述第二通信装置包括：

第二口令产生装置，用来根据从所述第一通信装置接收的信息，利用与第一口令产生电路一样的口令产生程序产生口令；以及

第二通信开始电路，用来响应该一致信号开始与所述第一通信装置的加密通信.

2.一种加密通信系统，其特征在于包括：

信息产生电路，用来根据一种不规则的信号产生用来生成每次通信连接都不相同的口令的有意义的信息;

口令生成器，用来根据所述信息利用口令生成程序生成口令;

判决电路，用来确定从另一个加密通信装置接收的口令与所述口令生成器输出的口令是否一致，若两口令一致，则输出一致信号，或者若所述两口令不一致，则输出不一致信号;

通信开始电路，用来响应该一致信号开始与另一个通信装置的加密通信。

3.按照权利要求 1 的装置，其特征在于：所述不规则信号至少是噪声信号或气候信号中的一种信号；所述口令生成器把所述不规则的信号数字化，根据所生成的数字数据产生随机数，确定所述随机数数据过去是否用过，若过去未用过，则将所述随机数数据作为所述信息输出。

4.一种加密通信系统，其特征在于包括：

第一加密通信装置和

第二加密通信装置；

所述第一加密通信装置包括：

信息产生电路，用来根据一种不规则的信号产生用来生成每次通信连接都不相同的口令的有意义的信息；

第一口令生成器，用来根据所述信息利用口令生成程序生成口令；

判决电路，用来确定从所述第二加密通信装置接收的口令与从所述第一口令生成器输出的口令是否一致，若两口令一致，则输出一致信号，或者若所述两口令不一致，则输出不一致信号；以及

第一通信开始电路，用来响应该一致信号开始与所述第二加密通信装置的加密通信；

所述第二加密通信装置包括：

第二口令生成器，用来根据从第一加密通信装置接收到所述信息、利用与所述第一口令生成器相同的口令生成程序生成所述口令；以及

第二通信开始电路，用来响应该一致信号开始与所述第一加密通信装置的加密通信。

5.一种加密通信系统，其特征在于包括：

第一加密通信装置；和

第二加密通信装置;

所述第一通信装置包括:

信息产生电路,用来根据一种不规则的信号产生用来生成每次通信连接都不相同的口令的有意义的信息;

第一口令生成器,用来根据所述信息利用口令生成程序生成口令;

判决电路,用来确定从所述第二加密通信装置接收的口令与从所述第一口令生成器输出的口令是否一致,若两口令一致,则输出一致信号,或者若所述两口令不一致,则输出不一致信号;以及

第一通信开始电路,用来响应该一致信号开始与所述第二加密通信装置的加密通信;

所述不规则信号至少是噪声信号或气候信号中的一种信号;所述第一口令生成器把所述不规则的信号数字化,根据所生成的数字数据产生随机数,确定所述随机数数据过去是否用过,若过去未用过,则将所述随机数数据作为所述信息输出;

所述第二加密通信装置包括:

第二口令生成装置,用来根据从所述第一加密通信装置接收的所述信息、利用与所述第一口令生成器相同的口令生成程序生成所述口令;以及

第二通信开始电路,用来响应该一致信号开始与所述第一加密通信装置的加密通信.

6.一种加密通信装置,其特征在于包括:

加密器,它包括多个不同的加密程序、加密用的随机数产生程序和用来产生时间信号或定时信号的计时器;

所述加密器根据由加密用的随机数产生程序指定的时间信号或定时信号,在不规则的时间间隔中选择这些加密程序中的一个,以此加密原文数据,并输出所产生的加密数据,而同时选择性地改变所选择的加密程序。

7.一种加密通信系统，其特征在于包括：

第一加密通信装置；和

第二加密通信装置；

所述第一加密通信装置包括：

加密器，它包括多个不同的加密程序、加密用的随机数产生程序和用来产生时间信号或定时信号的计时器；

所述加密器根据由所述加密用的随机数产生程序指定的所述时间信号或所述定时信号，在不规则的时间间隔中选择这些加密程序中的一个，以此加密原文数据，并输出所产生的加密数据，而同时选择性地改变所选择的加密程序；

所述第二通信装置包括：

解密器，它包括多个不同的加密程序、解密用的随机数产生程序和用来产生时间信号或定时信号的计时器；

所述解密器根据由所述解密用的随机数产生程序指定的所述时间信号或所述定时信号，在不规则的时间间隔中选择这些加密程序中的一个，以此对从所述第一加密通信装置接收的所述原文数据进行解密，并输出所产生的解密后的数据，而同时选择性地改变所选择的解密程序。

8. 一种储存使计算机能够控制口令产生过程的口令生成控制程序的记录介质，其特征在于：所述口令生成控制程序使所述计算机根据一种不规则的信号产生用来利用口令生成程序生成每次通信连接都改变的口令的有意义的信息，以便确定所述口令与从另一个通信装置接收的口令是否一致，若所述两口令一致，则输出一致信号，而若所述两口令不一致，则输出不一致信号；口令生成控制程序响应该一致信号执行关于开始与另一个通信装置的加密通信的控制过程。

9. 一种储存使计算机能够控制口令产生过程的口令生成控制程序的记录介质，其特征在于：所述口令生成控制程序使计算机接收用来利用口令生成程序产生每次通信连接都改变的口令的有意义的信

息；并且根据所述信息、利用口令生成程序产生口令；所述口令生成控制程序根据从另一个通信装置接收到的口令一致信号、执行关于开始与所述另一个通信装置的加密通信的控制过程。

10. 一种储存使计算机能够控制加密装置的加密控制程序的记录介质，所述加密装置包括多个不同的加密程序、加密用的随机数产生程序和用来产生时间信号或定时信号的计时器，其特征在于：所述加密控制程序使计算机响应由所述随机数产生程序所指定的所述时间信号或所述定时信号，在不规则的时间间隔中选择所述多个加密程序中的一个，并加密原文数据，而同时选择性地改变所选择的加密程序。

11. 一种储存使计算机能够控制解密装置的解密控制程序的记录介质，所述解密装置包括多个不同的解密程序、解密用的随机数产生程序和用来产生时间信号或定时信号的计时器，其特征在于：所述解密控制程序使计算机响应由所述随机数产生程序所指定的所述时间信号或定时信号，在不规则的时间间隔中选择所述多个解密程序中的一个，并对加密的数据进行解密，而同时选择性地改变所选择的加密程序。

12.一种在第一通信装置和第二通信装置之间进行加密通信的方法，其特征在于包括以下步骤：

在第一通信装置中，每一次建立通信时根据一种不规则的信号产生用来生成每次通信连接都不相同的口令的有意义的信息；

根据所述信息利用第一通信装置中的口令生成程序生成口令；

把所述有意义的信息发送给第二通信装置；

在第二通信装置中根据从第一通信装置发送来的信息，利用与第一通信装置中一样的口令产生程序产生口令；

把第二通信装置中产生的口令发送给第一通信装置；

在第一通信装置中确定从所述第二通信装置接收的口令与从所述第一口令生成电路输出的口令是否一致；以及

若两口令一致，则开始第一通信装置与第二通信装置之间的加密

通信.

13.按照权利要求 12 的方法，其特征在于还包括以下步骤：

若在所述判决步骤中所述两口令一致，则把一致信号发送给第二通信装置；以及

响应接收到的一致信号，在第二通信装置中开始与第一通信装置的加密通信。

说　明　书

根据通信双方的开始信息产生口令的加密通信系统

本发明涉及加密通信系统，更具体地说，涉及能够改进口令的产生和降低加密复杂性的加密通信装置。

为了通信和数据的安全，目前各种各样的加密系统已经投入实际使用。这些加密系统包括 DES(Data Encryption Standard，数据加密标准)系统和 RSA(Rivest, Shamir 和 Adleman)公共密钥加密系统。DES 系统是一个加密算法公开型，亦即移位和字符替换结合的公共密钥加密系统。RSA 公共密钥加密系统由于要进行庞大的计算，对大量数据的加密不实用。RSA 系统往往用于加密通信双方的核实和密钥的共享。

今天，各种卡，包括预付卡和电话卡的伪造是一个迫切需要改正的社会问题。另外，这个与计算机应用相联系的问题是未经授权的人往往窃取口令，意图闯入计算机和通信网络。尽管现有的计算机和通信系统为了安全目的进行了某种程度的加密，但是并非所有的系统或终端都配有先进的加密方案。另外，不求助于复杂的程序和复杂的电路配置先进的加密是不现实的。因此，小型的数据终端和装置难以实现先进的加密方法。

现在 IC(集成电路)卡由于有大量存储器容量而正在代替磁卡。使用 IC 卡可以整个地把日常生活所需的各种类型的信息，例如财务信息和个人信息管理起来。另外，有人建议把 IC 卡应用于电话卡、火车用的预付卡和 pachinko 和其他游戏用的预付卡。为了在与主机连接通信时确保上述信息的安全和保护 IC 卡免受窃听，甚至用这样的 IC 卡加密也极其重要。另外，这个加密必须以细小的装置加以实现。

为了通信和数据安全目的而在现代计算机通信系统上实现某些

加密方案，而且每一种方案都用数值和句子的复杂组合来实现．但是，如果是静态(不变的和简单的)数值和句子组合，那么，即使以复杂的方式把数值和句子组合起来，使用大容量和高速计算机也是可以把它破解的．

因此，本发明的目的是提供一种加密通信用的和在从一台与计算机网络相连的计算机或数据卡终端发送数据时能够确保数据先进的安全性、保护数据卡终端不被非法使用并防止加密数据被非法解密的系统和装置．

按照本发明，加密通信系统包括：第一通信装置，用来产生有意义的信息以产生每次通信连接都不相同的的口令；和第二通信装置，用来从第一通信装置收到信息时基于所述信息产生口令，并将所述口令送到第一通信装置．第一通信装置包括信息产生电路，用来根据不规则的信号产生所述信息．第一口令产生电路根据所述信息利用口令产生程序产生口令．判决电路用来确定从第二通信装置收到的口令是否与从第一口令产生电路输出的口令一致，若两口令一致则输出一致信号，而若它们不一致则输出不一致信号．第一通信开始电路响应一致信号开始与第二通信装置的加密通信．第二通信装置包括第二口令产生装置，用来根据从第一通信装置接收的信息利用与第一口令产生电路一样的口令产生程序产生口令．第二通信开始电路响应一致信号开始与第一通信装置的加密通信．

另外，按照本发明，加密通信系统包括第一加密通信装置和第二加密通信装置．第一通信装置包括信息产生电路，用来根据不规则的信号产生用来生成每次通信连接都不相同的口令的有意义的信息．第一口令生成电路根据所述信息利用口令生成程序生成口令．判决电路确定从第二加密通信装置接收的口令与第一口令生成电路输出的口令是否一致，若两口令一致，则输出一致信号，或者，若所述两口令不一致，则输出不一致信号．第一通信开始电路响应该一致信号开始与第二加密通信装置的加密通信．所述不规则信号至少是噪声信号或气

候信号中的一个．第一口令生成电路把所述不规则的信号数字化，根据所生成的数字数据生成随机数，确定所述随机数数据过去是否用过，若过去未用过，则将所述随机数数据作为所述信息输出．第二加密通信装置包括第二口令生成电路，用来在从第一加密通信装置收到所述信息时，利用与第一口令生成电路相同的口令生成程序生成所述口令．第二通信开始装置响应该一致信号开始与第一加密通信装置的加密通信。

另外，按照本发明，加密通信装置包括加密电路，后者包括：多个不同的加密程序；用于加密的随机数产生程序；以及计时器，用来产生时间信号或定时信号。加密电路根据由加密用随机数产生程序指定的时间信号或定时信号，在不规则的时间间隔中选择这些加密程序中的一个，以此加密原文数据，并输出所得加密数据，而同时选择性地改变所选择的加密程序。

另外，按照本发明，在储存允许计算机控制口令产生过程的口令生成控制程序的记录介质上，口令生成控制程序根据不规则信号使计算机产生有意义的信息，用来产生每次通信连接都改变的口令，以便利用口令生成程序产生口令、从而确定所述口令与从另一个通信装置接收的口令是否一致，若所述两口令一致，则输出一致信号，而所述两口令不一致，则输出不一致信号．口令生成控制程序响应该一致信号执行控制过程、以便开始与另一个通信装置的加密通信。

联系附图考虑以下的详细描述，本发明的目的和特征将变得更加清楚．附图中：

图 1 是一个方框图，示意地表示实施本发明的加密通信系统，尤其是表示数据终端卡装置与主机之间的加密方案；

图 2 是一个方框图，，与加密程序和基于对口令确认的解密程序一起，示意地表示包括在实施例中的生成口令用的特定配置；

图 3 是一个方框图，示意地表示构成包括在本实施例中的开始信息产生程序电路的随机数产生程序电路和随机数验证程序电路的特定

的配置;

图 4 是一个方框图，示意地表示开始信息产生程序电路更为具体的配置;

图 5 是一个方框图，示意地表示包括在构成本实施例的每一个数据终端卡装置和主机中的口令生成程序电路的特定配置;

图 6 是一个方框图，示意地表示也包括在本实施例中的数据加密电路的特定配置;

图 7 是一个方框图，示意地表示数据加密电路的更具体的配置;

图 8A 和 8B 是流程图，显示加密原文数据用的本实施例所特有的特定程序;

图 9A 和 9B 表示把字符转换成数值并用来执行图 8A 和 8B 所示程序的表;

图 10 表示图 8A 和 8B 加密程序中生成第一加密数据用的数值;

图 11 表示图 8A 和 8B 加密程序中生成第二和第 N 个加密数据用的数值;

图 12 表示加密数据在第一和第二计算机中如何同步和谐地随着时间的过去而变化;

图 13 表示一种特定的系统配置，它使第一和第二计算机能够通过从无线电波发送站接收校准用的基准无线电波而使它们的时间匹配;

图 14 表示数据终端卡装置的一种特定配置，它能够根据从无线电波发送站接收的基准无线电波来校准其时间.

在进入本实施例的详细描述之前，先描述按照本发明加密通信系统最佳实施例的原理. 说明性的实施例用一种任何时候都在动态地变化以致根本不能猜测解密方法的加密方法来代替传统的数值与正文(加密数据)的静态或不变的结合. 这种方法成功地阻止未经授权的人对加密数据进行解密. 例如，在个人计算机通信中，每一次通信连接 ID(识别)码或口令都无任何规则性地变化. 另外，过去用过的 ID 码或

口令不再使用. 采用这种配置， ID 卡和口令就能防止第三方的解密或非法使用。

两台计算机之间、例如数据卡终端和数据卡阅读器或网络系统之间的密码任何时间都在动态地变化. 所述码的这种改变的前提是，这两台计算机在开始时和在加密和解密过程中都彼此同步；否则加密数据就无法解密成原文。因此，加密侧的时间与解密侧的时间必须一致. 为此，时钟电路的时钟根据基准时间匹配. 可以利用从基准无线电波发送站或 GPS(全球定位系统)机基准时间的代表发出的无线电波信号中所含的高精度时间信号作为基准时钟.

在准备描述的实施例中，当两台计算机(例如，能够通过网络通信的数据卡终端和数据卡阅读器或两台计算机)保持数据通信时，它们各自以这样的方式控制加密过程，使得它们的口令和数据被加密，并防止窃听.

加密系数，亦即用于控制加密的信息和加密码是随着时间顺序地变化的。也就是说，本实施例总在利用程序序列改变加密方法. 这与传统的固定的或静态的加密方式形成鲜明的对照.

在两台计算机开始通信时，它们的程序的开始时间是匹配的，而加密程序则是变化的。同时，解密程序也随着加密程序的变化而变化.

加密用的数值随着时间的过去而动态地变化，因此，与从静态的加密产生的数值相比，解密就要困难得多了.

加密方法无规则地变化，而同时解密方法利用时间作为密钥与变化着的加密方法匹配。举例来说，加密方法相继出现的变化之间的时间间隔最好应该是不规则的，并根据随机数表的数值而变化.

最好作出这样的安排，使得解密时序可以调整，以便即使时钟略有偏差，也能确保解密.

参照附图的图 1，实施本发明的加密通信系统包括可以彼此通信的主机 1 和数据终端卡装置 2 . 数据终端卡装置(以下简称卡装置)2 是一种以 IC 卡的形式实现的电话卡、弹球盘(pachinko)游戏卡或类似的

预付卡．必要时，主机 1 可以用通信装置代替．主机 1 和卡装置 2 可以通过无线电通信系统或有线通信系统彼此连接．为了允许卡装置 2 和主机 1 利用加密数据保持通信，必须使卡装置 2 能够首先产生口令 401，并将其送往主机 1．若主机 1 确认所述口令，它就允许卡装置 2 与之保持加密通信．

说明性实施例的前提是每一次都替换口令，使得第三方不能窃取．另外，还要防止第三方预测产生口令的方法和机制．为了满足这些要求，说明性实施例产生完全无规则的口令．尤其是，卡装置 2 利用从主机 1 接收的无法预测的开始信息产生口令．

主机 1 包括开始信息产生程序 11，后者用来产生上述无法预测的开始信息．主机 1 把从开始信息产生程序 11 输出的开始信息 403 送往包括在卡装置 2 中的口令产生程序 21．同时，主机 1 使也建立在其中的口令产生程序 12(见图 2)产生口令．主机 1 使口令产生程序 11 根据无法预测的信息产生开始信息，而同时防止程序 11 输出同样的开始信息 403 两次或多次．当在卡装置 2 和主机 1 之间建立通道时，卡装置 2 的程序 21 根据从主机 1 接收到的开始信息产生口令 401．所述口令 401 从卡装置 2 送往主机 1 确认．若从卡装置 2 接收到的口令与主机 1 中产生的口令一致，则主机 1 确认它，而允许卡装置 2 与之保持加密通信．若所接收的口令与主机 1 中产生的口令不同，则主机 1 拒绝加密通信．

当从卡装置 2 送往主机 1 的口令 401 得到确认时，卡装置 2 把原文数据 411 加密，并将所得的正文数据 405 送往主机 1．同时，卡装置 2 使用在所述技术上全新的加密方法．特别是，卡装置 2 另外还包括数据加密 22，用来执行随着时间改变的不规则的控制．数据加密 22 以复杂的方式控制多个不同的加密程序，以执行随着时间改变的不规则的控制．加密正文数据 405 送往主机 1．图 2 的加密电路 14 被包括在主机 1 内，并对接收的正文数据解密，以便重构原文数据 413．

下面将参照图 2 描述用来根据所述确认产生口令以及加密和解密

程序的特定配置。正如所示的，主机 1 除了开始信息产生程序 11 和口令产生程序 12 以外，还有判决装置 13 和用来通过随着时间而改变的无规则控制而对加了密的数据解密 的数据解密装置 14．开始信息产生程序 11 包括随机数产生程序电路 111 和随机数验证程序电路 112．随机数产生程序电路 111 通过程序处理产生无法预测的随机数，然后根据所述随机数产生口令以具有预选位数的预选块的形式产生开始信息．随机数验证程序电路 112 通过程序处理确定上述开始信息过去是否已经用过．若所述开始信息是新的，程序电路 112 把开始信息作为有效的开始信息送往口令产生程序 12．同时，程序电路 112 把开始信息 403 送往卡装置 2 的口令产生程序 21．

口令产生程序 12 和 21 每一个都用所述开始信息作为用来重构产生随机数的逻辑电路的信息(协议)．举例来说，所述逻辑电路可以是 M 序列(最大长度移位寄存器序列)．另外，程序 12 和 21 中的每一个都用所述开始信息作为上述逻辑电路用以产生随机数的初始数据(初始值)．这两个程序 12 和 21 在配置上是彼此相同的，当向其提供相同的开始信息时，输出相同的口令．因此，可以确定卡装置 2 所产生的口令 401 与主机 1 产生的口令相同．

具体地说，当卡装置 2 的口令产生程序 21 从主机 1 接收到开始信息 403 时，它按照所述开始信息利用随机数产生程序重构用来产生随机数的逻辑电路．另外，程序 21 设置初始数据并用逻辑电路产生随机数．程序 21 从所得的随机数序列选择预定的位数，并将其作为口令送往主机 1 的判决装置 13．

在主机 1 中，口令产生程序 12 也按照所述开始信息并利用与卡装置 2 的程序电路 21 一样的随机数产生程序重构用于产生随机数的逻辑电路．然后，程序 12 设置初始数据并用逻辑电路产生随机数．程序 12 从所得的随机数序列选择预选位数，并将其作为口令送往判决装置 13．

判决装置 13 把从卡装置 2 接收的口令 401 与从程序 12 输出的口

令比较，看看它们是否相同．若所述两个口令不相同，则主机 1 不接受来自卡装置 2 的访问，产生不一致信号 407．若所述两个口令相同，则主机 1 把一致信号 409 送往卡装置 2 的数据加密装置 22．正如后面将要专门描述的，所述数据加密装置 22 执行随时间改变的不规则的控制．从判决装置 13 输出的一致信号 409 加在主机 1 的数据加密装置 14 上，使之开始对加了密的正文数据 405 进行解密．

在上述结构中，即使未经授权的人成功地窃取了卡装置 2 和主机 1 之间的所述口令产生开始信息 403，这个人也不能产生与主机 1 内产生的口令相同的口令，除非这个人得知口令产生程序 21 的口令产生方法．另外，即使未经授权的人窃取了口令 401，并试图用所述口令访问主机 1，主机 1 的判决装置 1 会确定所窃取的口令是不能接受的．这是因为主机 1 每一次卡装置 2 与主机 1 连接时都产生不可预测的口令．

尽管未经授权的人可能同时窃取了所述口令产生开始信息和与之相联系的口令，由于以下原因这个人也极难推算出口令和开始信息之间因果关系．卡装置 2 的口令产生程序 21 根据口令产生开始信息的一部分构造用来产生随机数的逻辑电路．所述逻辑电路利用所述开始信息的另一部分设置逻辑电路中的初始数据．结果，开始信息每改变一次，就构造一个新的逻辑电路，产生全新的随机数．因此对于未经授权的人来说，要猜测其规律性是极其困难的、并且消耗的时间长得无法实现．

有可能卡装置 2 被盗，因而口令产生程序 21 的程序被盗．有鉴于此，主机 1 最好应该能够管理分配给各个卡装置 2 的序列号．当卡装置 2 被盗时，主机 1 即以这样的能力删除在其中登记的卡装置 2 的序列号．以后当在被盗的卡装置 2 和主机 1 之间建立通道时，主机 1 命令卡装置 2 把它的序列号发送给主机 1．因为被盗卡装置 2 的序列号已经删除，所以，主机 1 不会向所述卡装置 2 发送用于产生口令的开始信息．

图 3 表示随机数产生程序电路 111 和随机数验证程序电路 112 的特定配置。在图 3 中，随机数产生程序电路 111 利用从自然现象衍生的信号产生用于开始信息 403 的随机数。正如所示，电路 111 包括空间噪声和气候数据收集电路 111a 、量化电路 111b 和块数值输出电路 111c 。在说明性实施例中，空间噪声和气候数据搜集电路 111a 用简单的天线捕获电磁波信号形式的空间噪声，并输出空间噪声信号。空间噪声是所需要的信号，这是因为它的振幅以同非周期性的自然随机数的相同的方式变化。另外，温度和湿度的变化类似于自然随机数，因为它们也是以不可预测的方式变化的。响应变化的温度和湿度的传感器（未示出）被包含在搜集电路 111a 中。所述搜集电路 111a 如图所示通过连接 421 向量化电路 111b 馈送空间噪声信号，以及所述传感器的代表瞬间温度和湿度、亦即气候数据的输出信号。

量化电路 111b 把输入的空间噪声信号和气候数据 421 量化，并输出相应的数字信号 423 。块数字输出电路 111c 把所述数字信号转换成数值块，并以此输出临时口令产生开始信息 425 。这个信息包括用来构造产生口令的逻辑电路的信息块和初始值数据块。把临时口令产生开始信息从电路 111c 馈送到随机数验证程序电路 112 。

随机数验证程序电路 112 检验从块数值输出电路 111c 接收的临时开始信息 425 。若临时开始信息适当，程序电路 112 将其作为准备实际使用的有效的口令产生开始信息 403 输出。具体地说，程序电路 112 具有重用判决电路 112a ，用来确定临时开始信息过去用过没有。只要临时开始信息过去未曾用过，重用判决电路 12a 就会将其作为有效的口令产生开始信息输出。这个开始信息储存在主机 1 中，用来验证将来出现的开始信息。

下面将参照图 4 描述图 3 所示开始信息程序 11 的更加具体的配置。如图所示，程序 11 包括天线 111a1 ，用来捕获空间噪声，并将所得空间噪声信号 431 馈送到包括在量化电路 111b 的模数转换器 (ADC)111b1 。温度传感器 111a2 检测主机 1 周围的温度，并将其转换

成温度电信号 433．湿度传感器 111a3 检测主机 1 周围的湿度，并将其转换成温度电信号 435．温度信号 433 和湿度信号 435 从传感器 111a2 和 111a3 分别输出，并馈送到 ADC 111b1．

ADC 111b1 把空间噪声信号、温度信号和湿度信号转换成为具有、例如一个样值 20 位的数字信号 437．用这 20 位数值信号，可以产生 2^{20}(=1,048,576)个不同的组合．从 ADC 111b1 输出的一个样值 20 位字长的数字信号 437 被送到块数字输出电路 111c，并以此转换成临时口令产生开始信息 425．具体地说，20 位中的 10 位用作构造随机数产生逻辑电路的信息，在所述情况下，其余 10 位用作初始值数据。若有必要，可以在以上 20 位上再加 α 位(随机数)。

从块数字输出电路 111c 输出的临时开始信息 425 被馈送到包括在重用判决电路 112a 中的一致性判决电路 112a1．信息表 112a2 列出所产生的及过去输出的口令产生开始信息。一致性判决电路 112a1 为了确定从块数字输出电路 111c 接收的临时开始信息 425 是否与列在表 112a2 中的过去的信息中的任何一个一致。若这个判决的答案是肯定的，则所述临时开始信息便被抛弃，不用来产生口令。若这个判决的答案是否定的，则判决 112a1 确定所述临时开始信息过去未曾用过。然后，判决电路 112a1 把这个所述临时开始信息作为有效的开始信息 403，并将其登记在所述信息表 112a2 中，以便这个有效的开始信息以后不被重用。

图 5 表示卡装置 2 的口令产生程序电路 21 或主机 1 的口令产生程序电路 12 的具体配置．如图所示，程序电路 12 或 21 一般都包括译码器 121 和随机数发生器 131．收到口令产生开始信息 403 时，译码器 121 对所述信息进行译码，然后把译码后的信息分成用来确定作为随机数发生器 131 的逻辑电路配置的数据(例如，"0010")和初始数据(例如，"101")．这些数据从译码器 121 馈送到随机数发生器 131．

随机数发生器 131 是 N 级的，M 序列发生电路，其中包括移位寄存器 122-124、开关 125，126，129 和 130 及"异"门("异")127

及 128．确定逻辑电路配置的数据选择性地使开关 125， 126， 129 和 130 接通或断开．具体地说，假定如图 5 所示，上述数据是"0010"，则译码器 121 的输出"0"使开关 125 断开，以此使移位寄存器 122 的输入端和“异”门 127 的输入端断开．这加上译码器 121 的另一个输入端为"0"使开关 129 断开的这一事实，使“异”门可以操作．类似地，译码器 121 的另一个输出端为"1"使开关 126 接通，以此连接移位寄存器 123 的输入端和“异”门 128 的输入端，而同时译码器 121 的另一个输出端为"0"使开关 130 断开．因此，“异”门 128 保持可操作．

假定，如图 5 所示，译码器 121 的初始数据输出是"101"．于是，数据"1"使移位寄存器 122 和 124 中的每一个置“1”，作为初始数据的一部分，而同时，数据"0"使移位寄存器 123 复位，作为初始数据的另一部分．

使用上述逻辑电路配置和初始数据，随机数发生器 131 就能够通过“异”门 130 的输出端输出 M 序列，具有 2^n-2(n 是移位寄存器的级数)长度的伪随机数序列．预定位数的伪随机数序列，例如 20 位(在十六进制表示中的 5 位数字)可以用作口令．这使得可以使用总共 2^{20}=1,048,576 个不同口令中的任何一个．

如上所述，当口令产生开始信息的位安排改变时，随机数发生器 131 的逻辑电路配置和在发生器 131 的移位寄存器中设置的初始数据随之改变．结果，就可以产生没有因果关系的随机数序列，允许口令具有可变的位安排．于是，未经授权的人便无法从口令产生开始信息预测口令，除非此人能够从开始信息推导出译码器 121 的译码方法．译码器 121 的译码方法是指，例如，多少位开始信息分配给初始数据，又多少位分配给逻辑电路配置．因此，第三方对口令的非法预测就可以排除，因为译码方法是变化的．

现将参照图 6，描述执行随时间变化的无规则控制的卡装置 2 的数据加密 22 的具体配置．如图所示，数据加密 22 具有加密器 221-

223、组合器 224 和随机数发生程序电路 225。加密器 221-223 的每一个都用特定的随机数发生电路对原文数据进行加密。组合器 224 把加密器 221-223 输出的加密数据 441-443 组合起来，并输出组合后的数据 405。随机数产生程序电路 225 包括随机数发生器，并选择性地使加密器 221-223 中的任何一个按照控制信号 445-447 随着时间而无规则地操作。

例如，上述程序电路 225 使加密器 221 以 t1 和 t4 的时间周期操作，使加密器 222 以 t2 和 t5 的时间周期操作，使加密器 223 以 t3 和 t6 的时间周期操作；周期 t1, t2 和 t3 彼此不同，而周期 t4, t5 和 t6 也是如此。这种控制可以使加密器 221-223 可以被选择，并无规则地操作，实现全新的复杂的加密。解密侧将配置随机数产生程序，后者用来执行与程序电路 225 的随时间无规则变化的控制相反的控制，以便把加密的数据 405 解密。

图 6 的数据加密 22 更加具体的配置示于图 7。如图所示，加密器 221 具有随机数发生器 221b 和“异”门 221a。“异”门 221a 利用随机数发生器 221b 输出的随机数序列 448 对原文数据 411 加密。随机数产生程序电路 225 包括随机数发生器 225a。从随机数发生器 225a 输出的随机数 445 使随机数发生器 221b 在例如图 6 所示的时间周期 t1 和 t4 运行。

加密器 222 具有随机数发生器 222b 和“异”门 222a。“异”门 221a 利用随机数发生器 222b 输出的随机数序列 449 对原文数据 411 加密。从随机数发生器 225a 输出的随机数 446 使随机数发生器 222b 在例如图 6 所示的时间周期 t2 和 t5 运行。另外，在加密器 223 中，“异”门 223a 利用随机数发生器 223b 输出的随机数序列 450 对原文数据 411 加密。从随机数发生器 225a 输出的随机数 447 使随机数发生器 223b 在例如图 6 所示的时间周期 t3 和 t6 运行。

随机数发生器 221b, 222b 和 223b 每一个都以特定的随机数发生方法、特定的随机数周期运行，因此可以用图 5 所示的随机数发生器

131 实现. 包括在程序 225 电路中的随机数发生器 225 可以包括用来输出图 6 所示的输出控制信号 445-447 的随机数发生器和定时信号发生器.

现参照图 8A 和 8B 描述加密原文数据用的另一个特定的程序. 假定步骤 S10 的原文是发音为"ho-n-ji-tsu-wa-se-i-te-n-na-ri"的日文字符序列(平假名). 每一个音节相当于一个日文字符或平假名. 图 9A 和 9B 表示具体的字符至数字值转换表 TB1 . 程序开始于用转换表 TB1 把上述原文数据转换成数值序列 A1(步骤 S20). 结果, 如图 10 所示, (a)用数值序列"39, 55, 21, 56, 35, 23, 11, 28, 55, 30, 49"代替字符序列"ho-n-ji-tsu-wa-se-i-te-n-na-ri".

然后, 把某个常数、例如 46 加到每一个数值 A1 上, 以便产生数值序列 A2(步骤 S30). 如图 10 , (b)所示, 所述相加产生数值序列"85, 101, 67, 102, 81, 69, 57, 74, 101, 76, 95". 若有必要, 上述常数可以通过利用加密程序的控制而作不规则变化.

为了把数值 A2 的数字位数限制为 2 , 从大于等于 50 的数值 A2 减去 50 . 结果, 如图 10 , (c)(步骤 S40)所示, 得出数值序列(A2, A3) " 35, 51, 17, 52, 31, 19, 7, 24, 51, 26, 45 " . 若有需要, 要减的数值 50 可以用随机数表改变, 或者可以把随机数表中所列的数值乘适当次方.

然后, 从原来数值序列 A1 选择特定的前导块 B3(39, 55, 21)(步骤 S50). 构成块 B3 的数值"39", "55"和"21"分别加上序列(A2, A3)的前导的 3 个数值, 亦即, "35", "51"和"17". 通过顺序将块 B3 移位、用序列(A2, A3)的所有其他数值重复这种操作, 一次 3 个数值, 以产生数值序列 A4(步骤 S60). 所得序列 A4 , 如图 10 , (d)所示, 为"74 , 105 , 38 , 91 , 86 , 40 , 46 , 79 , 72 , 65 , 100". 换句话说, 块加密是用序列(A2,A3)的每 3 个数字字符执行. 若有必要, 块 B3 的数值"39", "55"和"21"可以根据加密程序改变, 或者改变块 B3 的长度.

再次用 50 减序列 A4 中大于等于 50 的数值，以此产生数值序列(A4， A5)(步骤 S70)。如图 10，(e)所示，所得序列(A4， A5)为"24，56， 38， 41， 36， 40， 46， 29， 22， 15， 50)。序列(A4，A5)可以作为第一加密数据输出。从序列 A4 减去的数值 50 可以利用随机数表改变，或者随机数表中的数值可以根据需要上升到适当的幂次。

另外，在例如， 1 秒过去时，在步骤 S50 选择的相继的块 B3(39，55， 21)中的一个不规则地移位。

如图 11，(b)所示，所得数值序列为，例如，"21， 39， 55，39， 55， 21， 39， 55， 21， 39， 55"。这些数值或移位块 SF(步骤 S80)分别加到步骤 S40 所产生的数值序列(A2， A3)上，并示于图 11，(a)。结果，(步骤 S90)产生数值序列 A6"56， 90， 72， 91，86， 40， 46， 79， 72， 95， 100"。

用数值 50 去减上述序列 A6 中大于等于 50 的数值。如图 11，(d)(步骤 S100)所示，这产生数值序列(A6， A7)"6， 40， 22， 41， 36，40， 46， 29， 22， 45， 50"。这个序列(A6， A7)可以作为第二加密数据输出。若有必要，从序列 A6 减去的数值 50 可以利用随机数表改变，或者随机数表中的数值可以根据需要上升到适当的幂次。

假定， N 移位块 SF 是在 N 秒过去时移位的，而如图 11，(e)所示，把所得序列"N,...N, 39, 55, 21, 39, 21, 55, 39"加到图 11，(a)序列(A2， A3)上。然后，如图 11，(f)所示，产生序列 A8"XN...ZN, 70, 74, 28, 63, 106, 47, 84"。从上述序列 A8 数值中大于等于 50 的数值减去 50。这产生图 11，(g)所示的序列"XN...ZN, 20, 24, 28, 13, 56, 47, 34"。这个序列可以作为第 N 次加密数据输出。若有必要，从序列减去的数值 50 可以利用随机数表改变，或者随机数表中的数值可以根据需要上升到适当的幂次。

解密侧通过第一次至第 N 次加密数据执行与加密程序相反的程

序，对第一次至第 N 次加密数据解密。为此目的，解密侧还使用图 9A 和 9B 所示的转换表，开始反处理程序。解密程序与加密程序同步。

第一和第二计算机最好使用下载时间作为基准、达成关于每次下载加密程序和代表动态加密变化规则的程序以及开始加密程序的通信协议。作为加密密钥的数值要随时随地顺序地改变。

关于更复杂的加密，数据可以相乘，然后上升到适当的幂次，在这种情况下，加密可以用立方根倒数实现。作为另一方案，原文可以用数目上等于构成正文的字符的密钥加密。

相继两次变化之间的时间间隔(例如，秒)是随机的，利用，例如列于随机数表中的数值改变。另外，随机数表各个数值可以上升到适当的幂次，并用作预选单位基础的上述时间间隔，另外，用来乘以所述数值或加密的密钥。也就是说，为了乘以数值，从随机数表选择的时间变化和加密正文的密钥最好应该彼此保持一致。

若第一计算机的时间与第二计算机的时间匹配，则加密程序和解密程序可以彼此同步。例如，如图 12 所示，若第一计算机的加密数据与第二计算机的加密数据匹配，而同时随着时间推移保持同步，则可实现加密通信。即使第三计算机成功地对图 12 所示的加密数据中任何一个进行解密，它也不能利用解密数据，因为所述数据已经被另一个加密数据代替了。

图 13 表示使预期要进行加密通信的第一计算机和第二计算机时间匹配的具体实现。如图所示，第一和第二计算机 1Aa 和 1Ab 分别各自配置基准波接收器 1A1 ，用来接收从适合于时间校准的发射站 3A 或全球定位系统（ GPS ）卫星发射的基准无线电波。在日本，例如，基准无线电波接收器可以周期性地接收日本邮电通信部控制的原子钟(误差为 300,000 年 1 秒)产生的基准无线电波。这种基准无线电波可以用来校正各个计算机的计时器，以便校正译码数据周期性变化的任何误差。图 14 表示达到上述目标的比较具体的系统配置。如图所示，数据终端卡装置 2A 包括天线 C1 、无线电波接收器 C2 、 RAM(随机存

取存储器)或工作区 C4 、高速存储器 C5 、可编程 ROM(只读存储器)C6、电源 C7、计时器 C8、外界连接电路 C9、显示器 10 和 CPU(中央处理单元)C11 。

天线 C1 和无线电波接收器 C2 最好应该从用于数据时间校正的无线电波发射站 11 接收基准无线电波信号，使计时器任何时间都保持正确。高速存储器 C5 最好应该储存口令产生程序、加密程序和用于与其他装置通信的通信程序。

当计时器 C8 慢了并使数据出错时，用高速计算机确定直到正确时间之前加密数据的变化，以便把加密数据向正确时间的加密数据推进。例如，当计时器快时，数值将通过程序校正到正确时间的数值。

当卡装置 2A 用电池供电时，装置 2A 可能由于电池消耗而接收无线电波失败，在计时器 C8 中引入了误差。有鉴于此，在最后一次接收无线电波的时间出现的加密用时间和数值可能已储存在高速存储器或类似的能够不求助于电池而能储存的半导体存储器。然后，当卡装置 2A 再一次使能无线电波接收器时，高速计算由卡装置 2A 的加密算法根据恢复时间执行，以便把数值进到正确时间的数值。

在计算机通信中，由于网络通信，数据安全性是极关重要的问题。今天可以得到的安全性太差了，尽管过去提出了各种各样的处理方案，仍旧无法结束电话卡、弹球盘（ pachinko ）游戏卡和其他数据的非法使用。静态(不变的和简单的)加密系统涉及将来会被未经授权的人译码的因素。相反，动态变化的安全系统使未经授权的人非法获得加密数据以便将其解密变得不现实了，因为加密方法每时每刻都在变化。

即使未经授权的人把加密方法的变化规则译码了，此人无法找到开始时间，因此无法搞清楚何时使用从加密数据推算出来的加密密钥。虽然未经授权的人可以对某个时间的数值译码，但是此人无法检测到表示随时间变化的规则的数值或者加密规则，因为所述数值每时每刻都在变化。

这成功地保护计算机网络免受非法使用，从而为健全的计算机数据通信作出重大贡献.

总而言之，在本发明的加密通信系统中，第一通信装置产生用于生成每次通信连接都变化的无法预测的口令的有意义的信息．第二通信装置根据上述信息产生口令，并将其发送到第一通信装置．若口令与第一通信装置产生的口令一致，则在这两个通信装置之间保持加密通信．这成功地防止未经授权的人非法使用.

另外，原文数据用所选择的并根据时间信号以不规则的时间间隔改变的不同的多个程序中的一个进行加密．因此，用简单的配置，就可以实现复杂得足以使第三方不能接触正文数据的加密.

因此，在属于开放的网络的计算机之间或在数据卡终端保持加密通信时，就能够确保数据的安全性，并使第三方极其难以非法使用、例如数据卡终端。

1997 年 5 月 20 提交的日本专利申请 No.129405/1997 的全部公开内容，包括说明书、权利要求书、附图和摘要全部包括在本文中作为参考.

尽管已经参考说明性实施例对本发明作了描述，但本发明不限于所述实施例．本专业的技术人员可以在不离开本发明的范围和精神的情况下，对所述实施例进行变更或修改。

说 明 书 附 图

图. 1

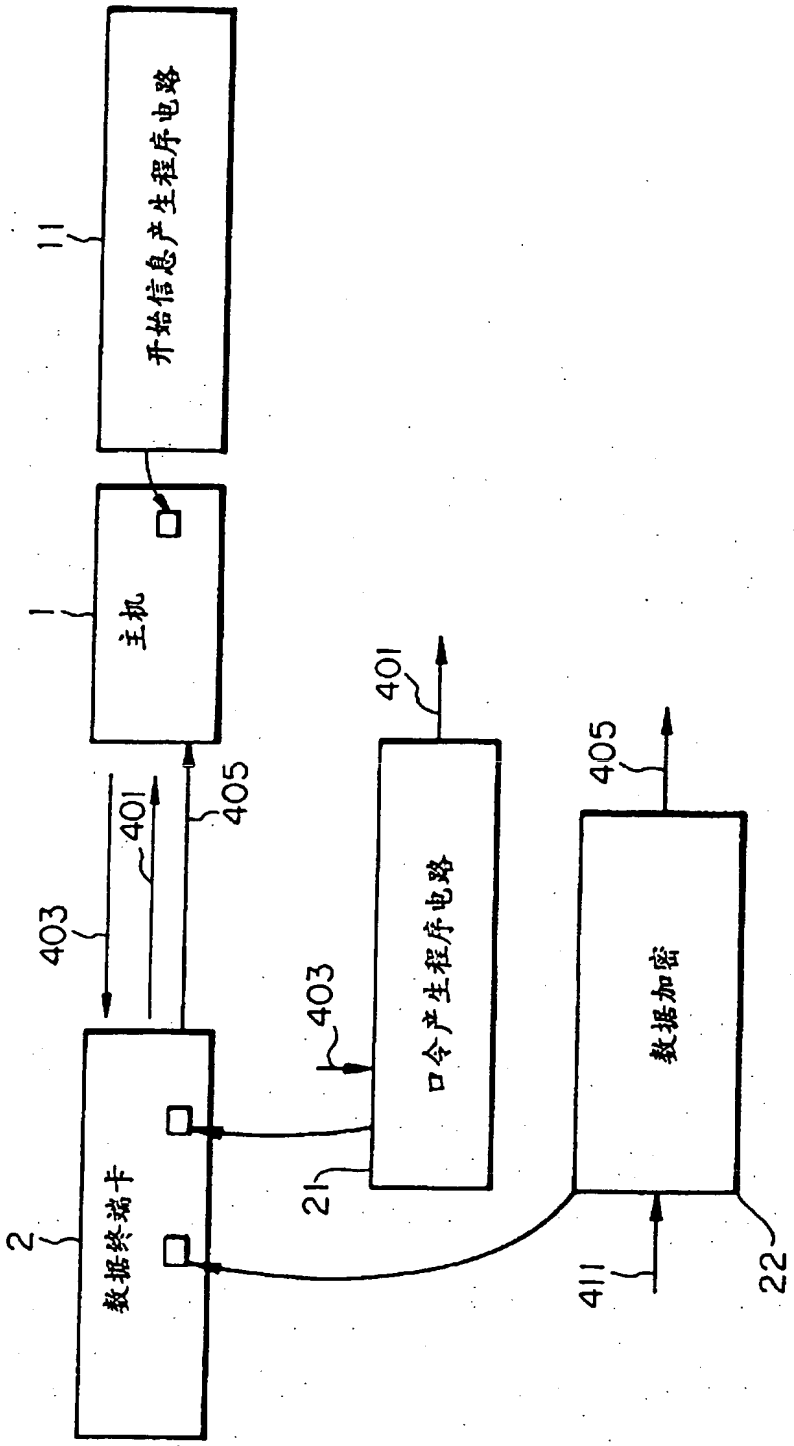

开始信息产生程序电路
11
主机
1
401
405
403
401
403
口令产生程序电路
21
405
数据加密
411
22
数据终端卡
2

图. 2

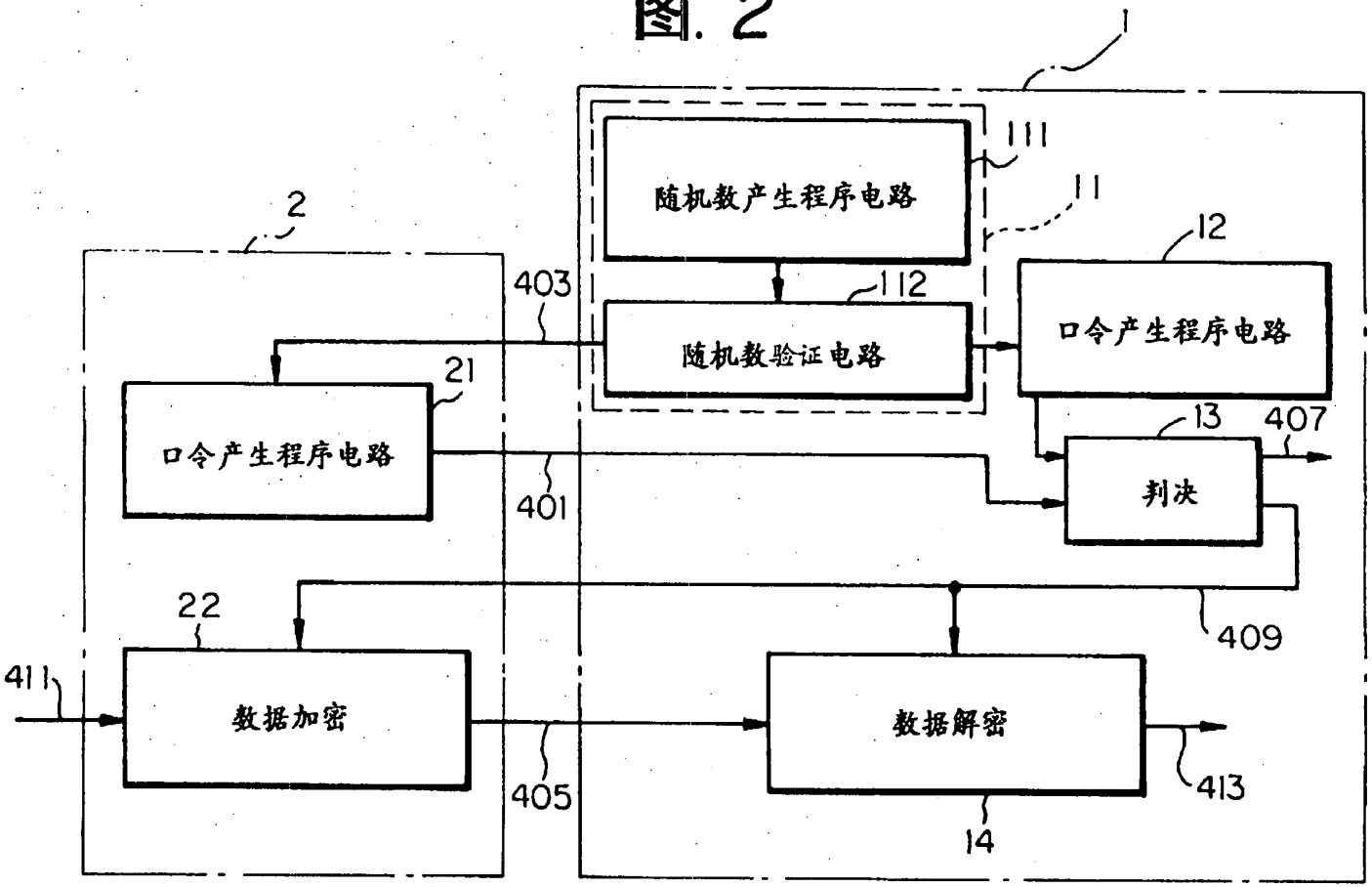

1
111
随机数产生程序电路
11
2
12
403
112
随机数验证电路
口令产生程序电路
21
13
407
口令产生程序电路
判决
401
22
409
411
数据加密
数据解密
405
413
14

图. 3

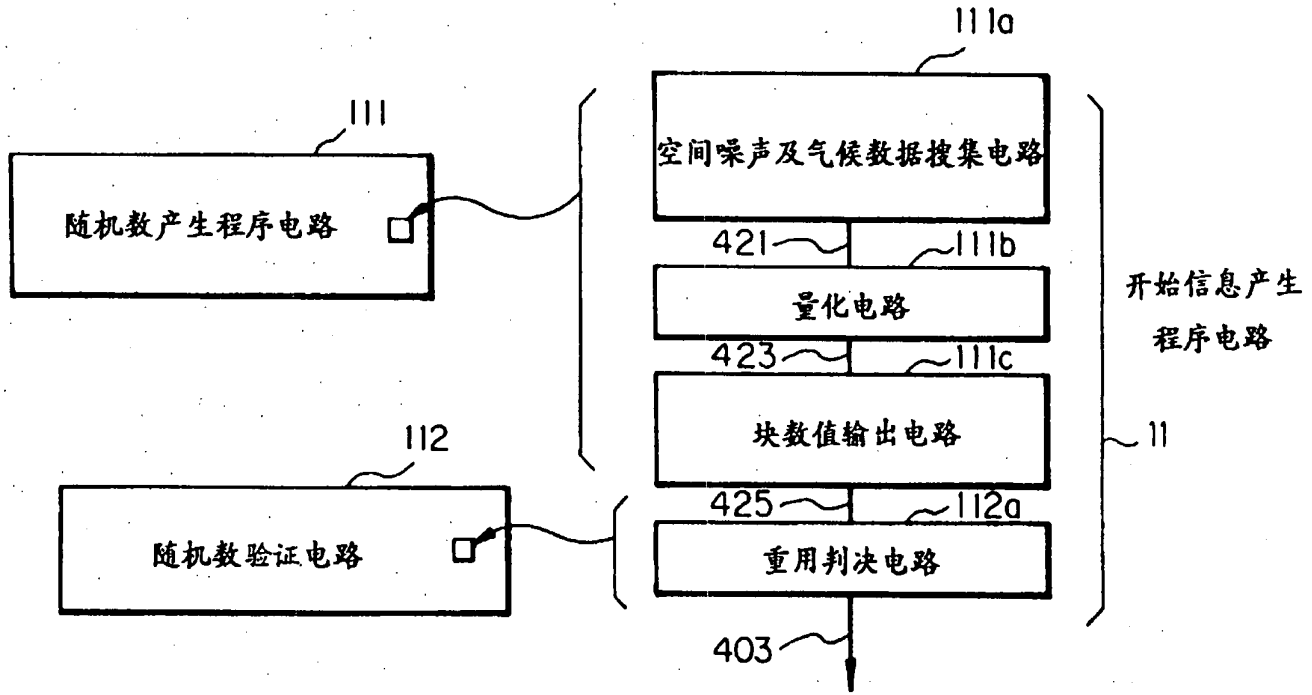

111a
空间噪声及气候数据搜集电路
111
随机数产生程序电路
421
111b
量化电路
423
111c
块数值输出电路
开始信息产生
程序电路
112
随机数验证电路
425
112a
重用判决电路
11
403

图. 4

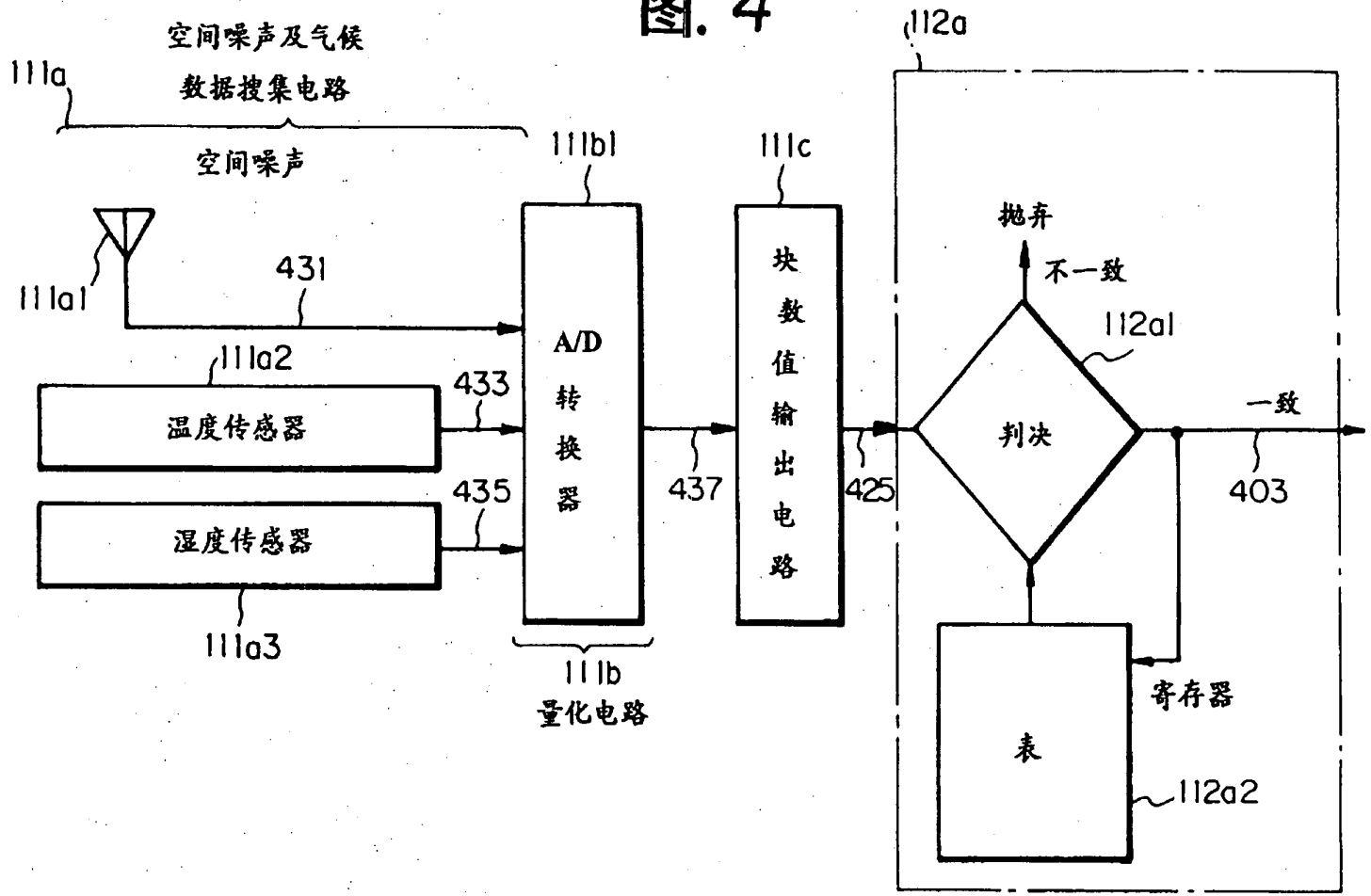

空间噪声及气候
数据搜集电路
111a
空间噪声
111a1
431
111a2
温度传感器
433
湿度传感器
435
111a3
111b1
A/D
转
换
器
111b
量化电路
437
111c
块
数
值
输
出
电
路
425
112a
抛弃
不一致
112a1
判决
一致
403
寄存器
表
112a2

图. 5

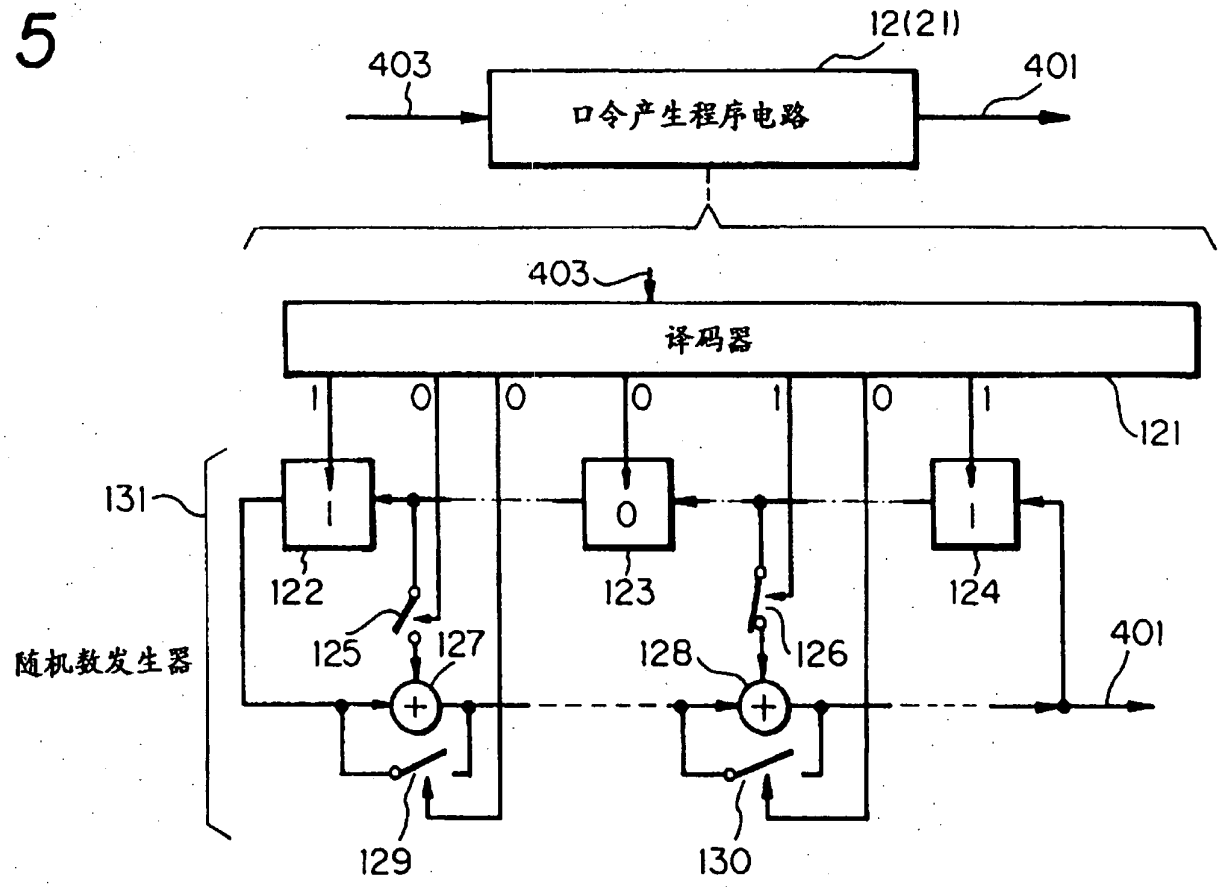

12(21)
403
401
口令产生程序电路
403
译码器
1
0
0
0
1
0
1
121
131
1
0
1
122
123
124
125
127
128
126
401
随机数发生器
129
130

图. 6

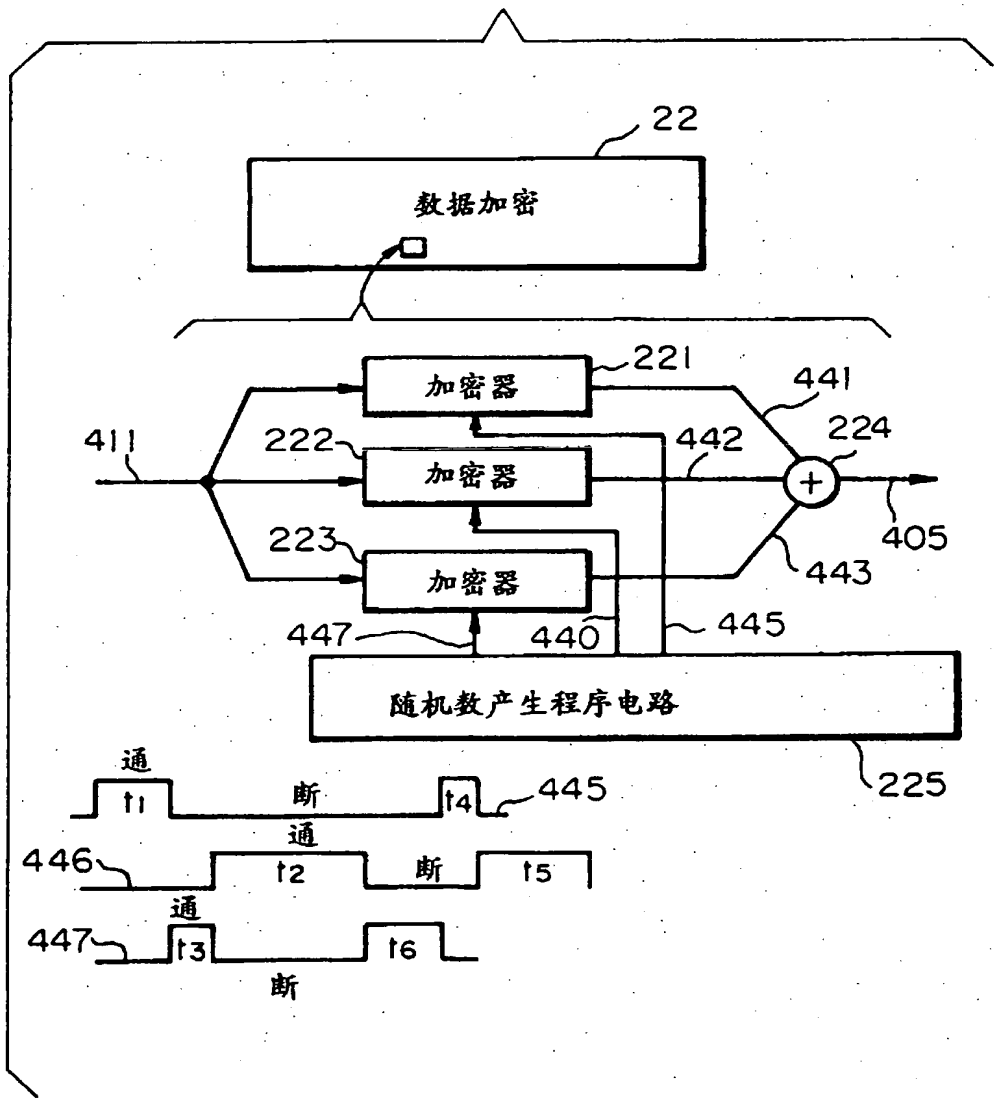

22
数据加密
221
加密器
441
411
222
加密器
442
224
223
加密器
405
443
447
440
445
随机数产生程序电路
225
通
t1
断
t4
445
446
通
t2
断
t5
通
447
t3
t6
断

图. 7

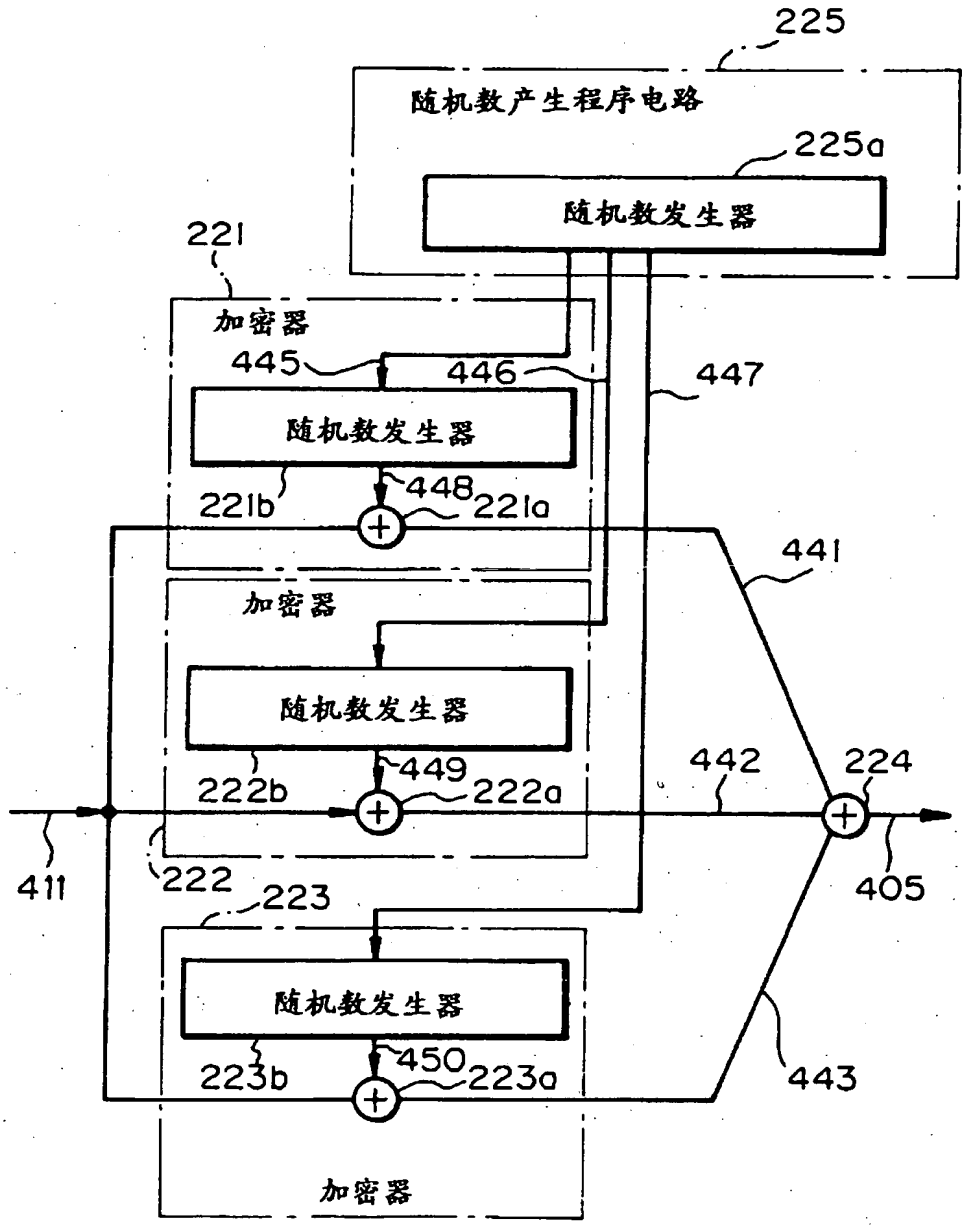

225
随机数产生程序电路
225a
随机数发生器
221
加密器
445
446
447
随机数发生器
221b
448
221a
441
加密器
随机数发生器
222b
449
222a
442
224
411
222
405
223
随机数发生器
223b
450
223a
443
加密器

图. 8A

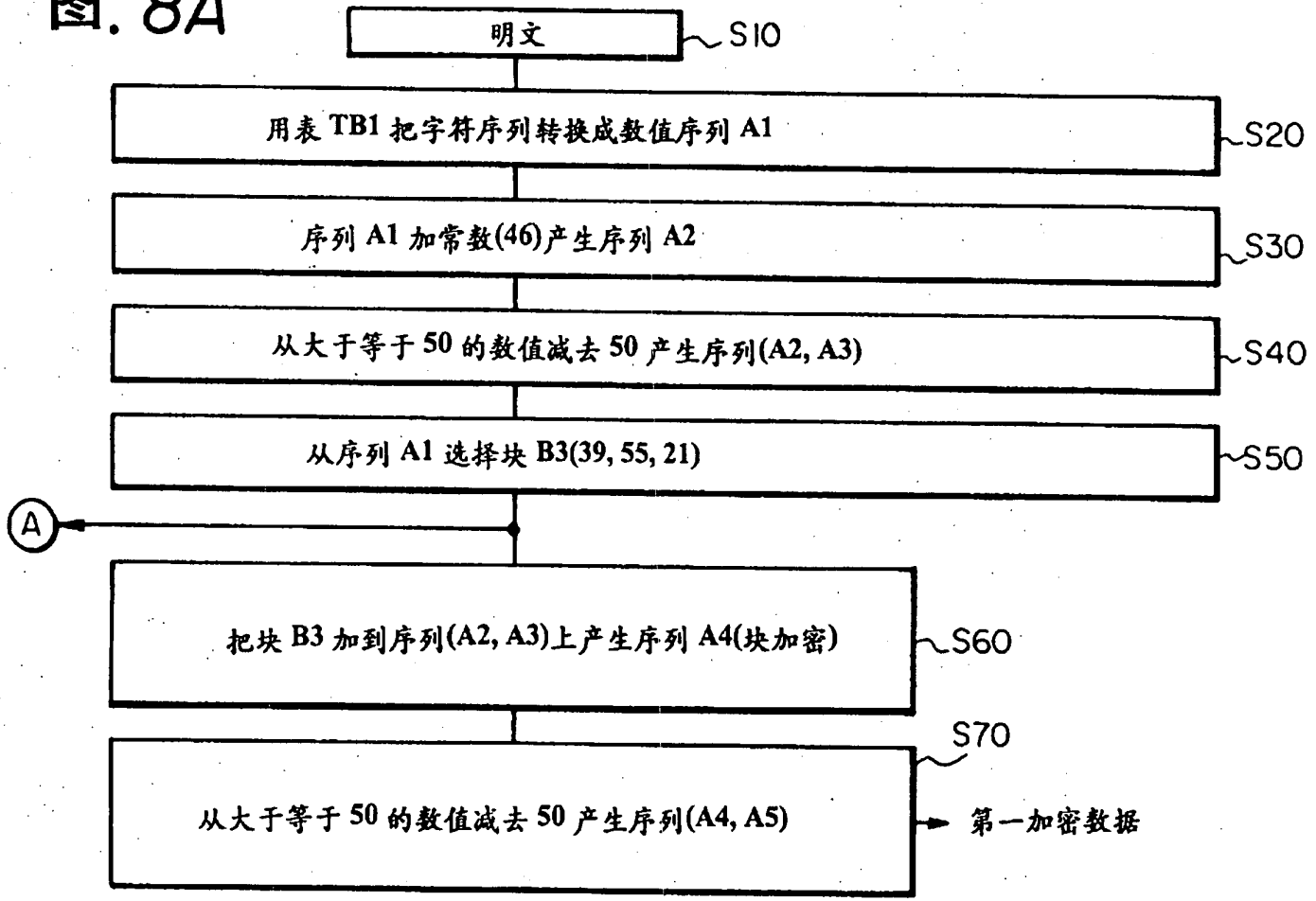

明文
S10
用表 TB1 把字符序列转换成数值序列 A1
S20
序列 A1 加常数(46)产生序列 A2
S30
从大于等于 50 的数值减去 50 产生序列(A2, A3)
S40
从序列 A1 选择块 B3(39, 55, 21)
S50
A
把块 B3 加到序列(A2, A3)上产生序列 A4(块加密)
S60
S70
从大于等于 50 的数值减去 50 产生序列(A4, A5)
第一加密数据

图. 8B

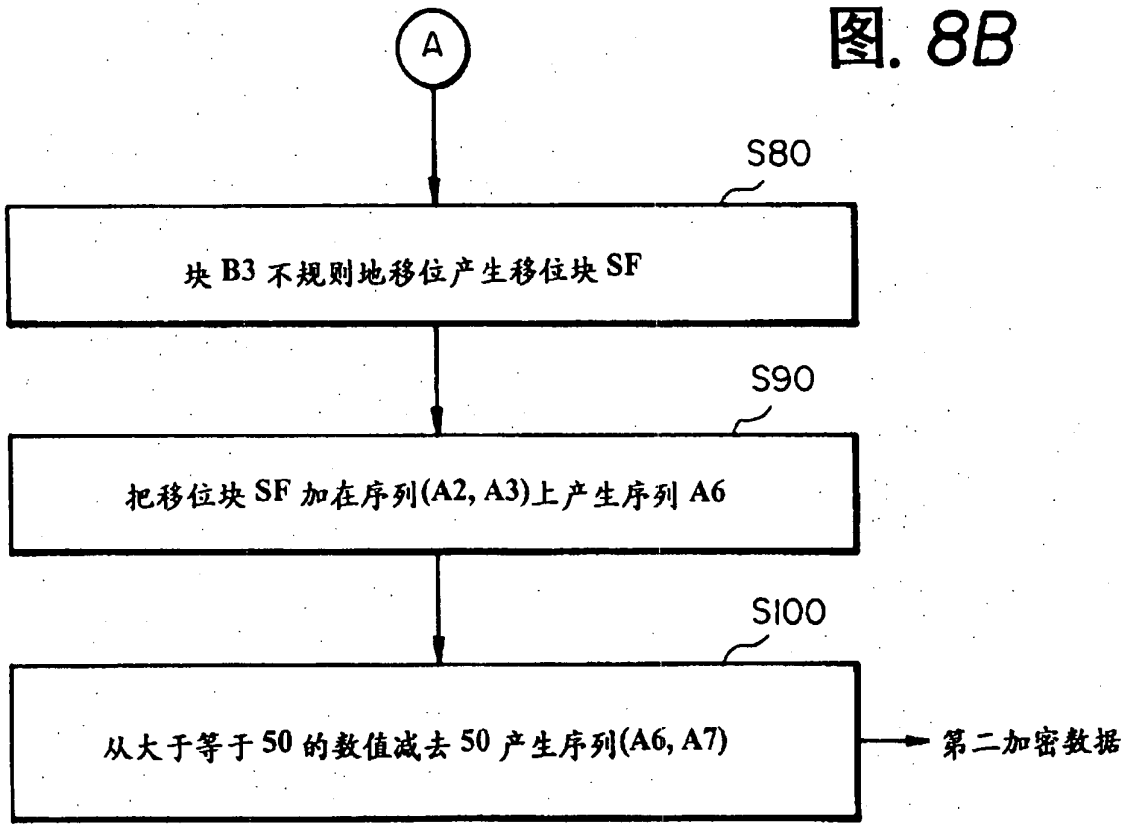

A
S80
块 B3 不规则地移位产生移位块 SF
S90
把移位块 SF 加在序列(A2, A3)上产生序列 A6
S100
从大于等于 50 的数值减去 50 产生序列(A6, A7)
第二加密数据

图. 9A

图 9

图 9A	图 9B

字符	数值	字符	数值
0	00	5	05
1	01	6	06
2	02	7	07
3	03	8	08
4	04	9	09
SA	20	TA	25
SHI	21	CHI	26
SU	22	TSU	27
SE	23	TE	28
SO	24	TO	29
MA	40	YA	45
MI	41	YU	46
MU	42	YO	47
ME	43		
MO	44		

图. 9B

字符	数值	字符	数值
A	10	KA	15
I	11	KI	16
U	12	KU	17
E	13	KE	18
O	14	KO	19
NA	30	HA	35
NI	31	HI	36
NU	32	HU	37
NE	33	HE	38
NO	34	HO	39
RA	48	WA	53
RI	49	WO	54
RU	50	N	55
RE	51	°	56
RO	52	、	57

图. 10

(a) 转换成数值

HO	N	JI	TSU	WA	SE	I	TE	N	NA	RI
39	55	21	56	35	23	11	28	55	30	49

(b) 加常数 46 作为加密密钥

85	101	67	102	81	69	57	74	101	76	95

(c) 减 50 把位数限制为 2

											2
35	51	17	52	31	19	7	24	51	26	45	

原来的数值

(a) 39	55	21	56	35	23	11	28	55	30	49	
39	55	21	移位并一次加 3 个数值								
(c) 35	51	17	52	31	19	7	24	51	26	45	

块数值

39	55	21	39	55	21	39	55	21	39	55

(d) 相加后的块数值

74	106	38	91	86	40	46	79	72	65	100

(e) 减 50 而给出的加密后数值

										50
24	56	38	41	36	40	46	29	22	15	50

图.11

(a)	一秒移位一块并相加										
	35	51	17	52	31	19	7	24	51	26	45
(b)	21	39	55	39	55	21	39	55	21	39	55
(c)	总和										
	56	90	72	91	86	40	46	79	72	95	100
(d)	减50而给出的加密后数值									50	
	6	40	22	41	36	40	29	22	45	50	
(e)	在N秒后移位N块并相加										
	35	51	17	52	31	19	7	24	51	26	45
	N----------			-N	39	55	21	39	55	21	39
(f)	总和										
	XN----------			-ZN	70	74	28	63	106	47	84
(g)	减50而给出的加密后数值									50	
	XN ----------			ZN	20	24	28	13	56	47	34

图. 12

第一计算机	
时间	加密数据
N1	0100110110
N2	0100110111
N3	0100111111
N4	0100000001
N5	0101010010

第二计算机	
时间	加密数据
N1	0100110110
N2	0100110111
N3	0100111111
N4	0100000001
N5	0101010010

图. 13

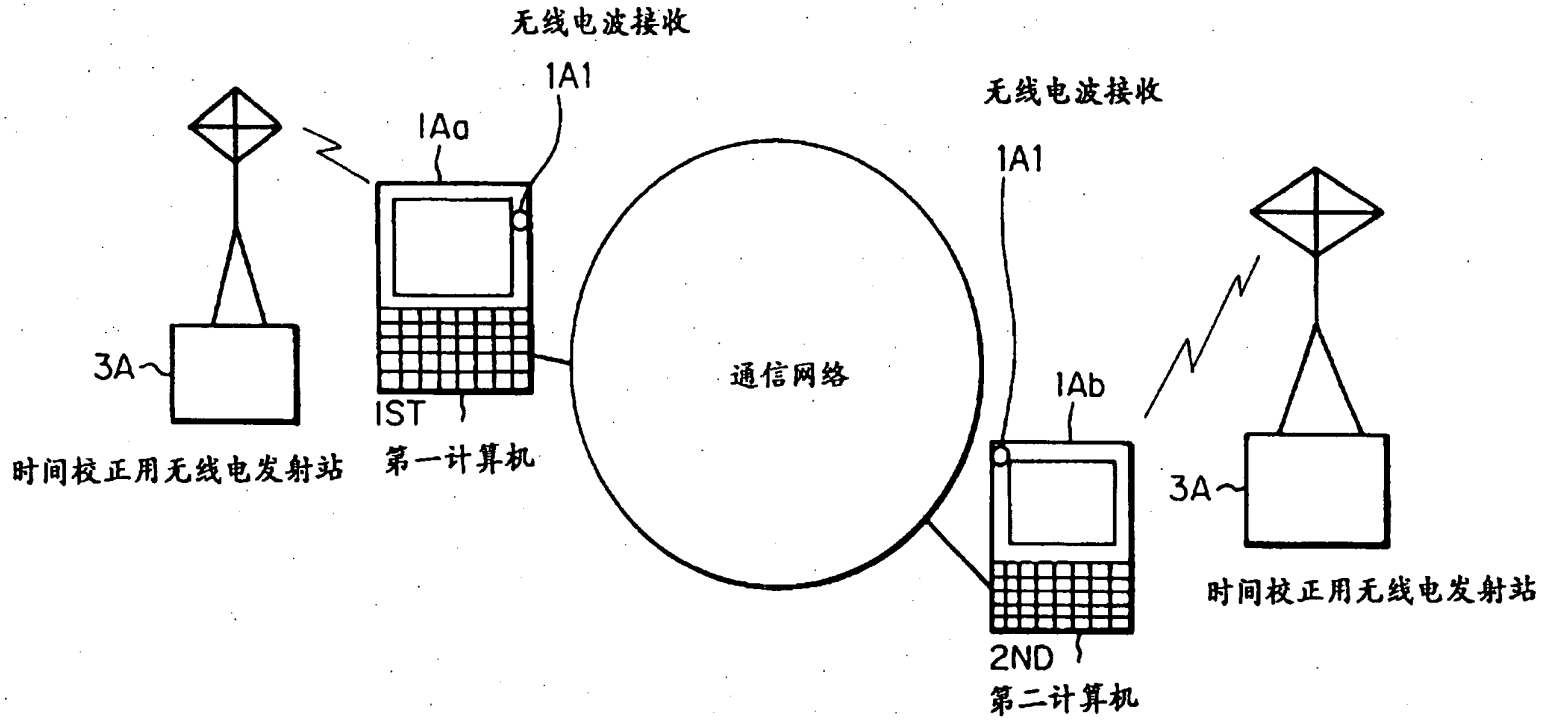
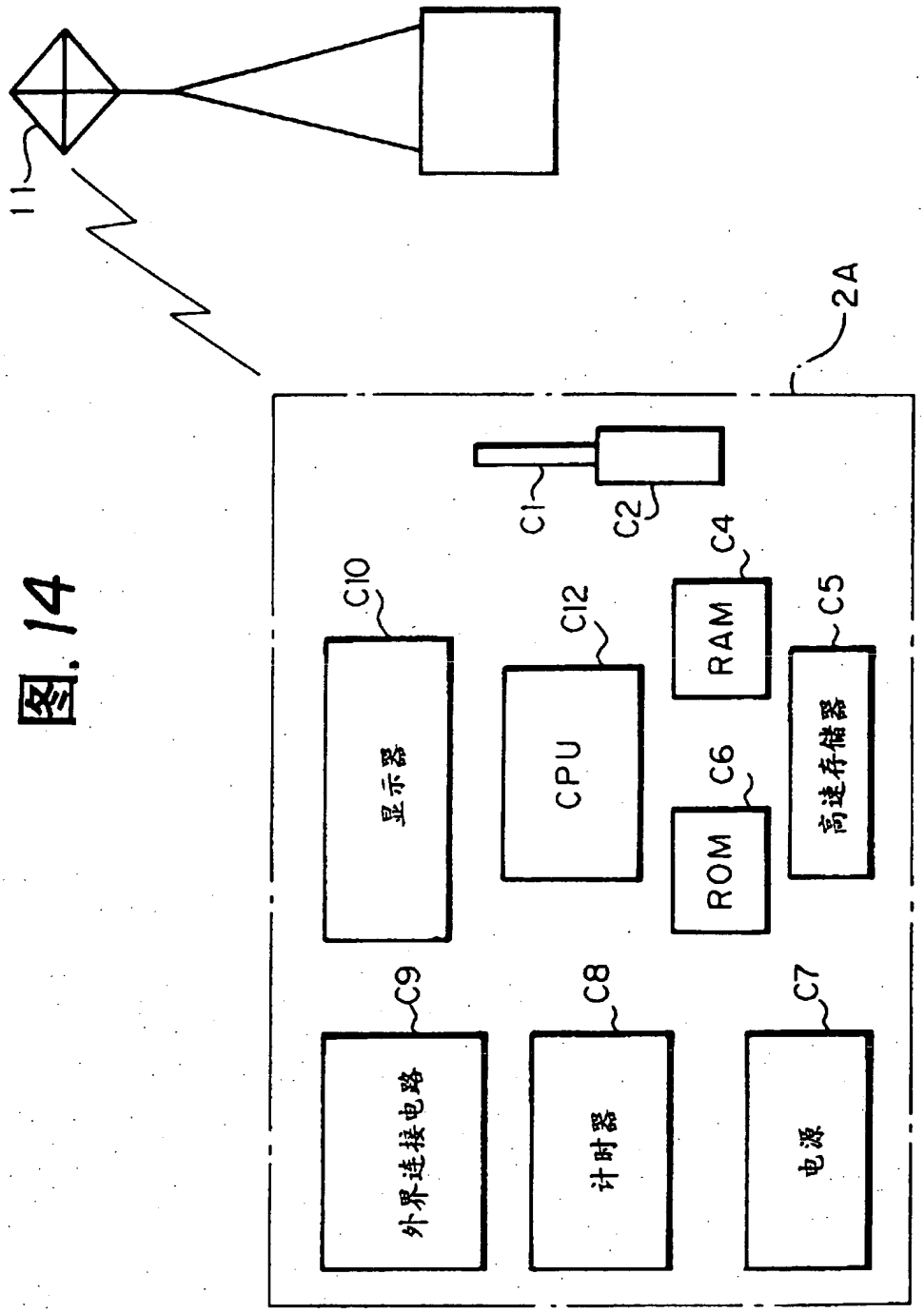

无线电波接收
1A1
1Aa
无线电波接收
1A1
3A
通信网络
1Ab
3A
1ST
2ND
时间校正用无线电发射站
第一计算机
第二计算机
时间校正用无线电发射站

图. 14


11
2A
C1
C2
C4
C5
C10
C12
RAM
显示器
CPU
C6
ROM
高速存储器
C9
C8
C7
外界连接电路
计时器
电源